# Colored Image Watermarking Technique Based on HVS using HSV Color Model

Piyush Kapoor[1], Krishna Kumar Sharma[1], S.S. Bedi[2], Ashwani Kumar[3],
[1] Indian Institute of Information Technology, Allahabad
[2] MJP Rohilkhand University, Bareilly.
[3] Infosys
Email: piyushkapoor7@yahoo.com, krisshna.sharma@gmail.com, erbedi@yahoo.com, ashwani_kumar09@infosys.com

*Abstract*— **The Human Visual System is found to be less sensitive to the highly textured area of the image. Moreover, in all colours the blue is least sensitive to the HVS (Human Visual System). While working on colored images when using the mathematical and biological models of HVS, the preferred colour model must be HSV (Hue, Saturation and Value) colour model rather than RGB colour model because it most closely defines how the image is interpreted by HVS. The high visual transparency in the technique is achieved by making use of highly textured block in luminance channel for watermark insertion. Moreover, the choice of selecting appropriate area for watermark insertion is also influenced by making use of 'Hue' property of the image in the chrominance channel to enhance the visual transparency even more. Watermark is made highly robust against different types of attacks by performing the watermark insertion in transformed domain and making use of the transformation functions such as DWT, DCT and SVD. The results demonstrated the robustness of the technique against various types of attacks and comparison through aforesaid results the technique is proven to be more robust against previous techniques making use of HSI colour model.**

*Index Terms*— **HSV color model, SVD, Human Visual System**

## I. Introduction

Digital storage and transmission is the major trend of handling information. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. In 2000 [1] used the histogram of 'value' or 'intensity' component of HSV color space to find out most appropriate area to insert the watermark. The basic idea of this technique is to eliminate (or reduce), in a controlled manner, groups of grey levels, taking care to preserve the visual appearance of the image [2]. The major disadvantage of the above technique that it is vulnerable to histogram specification attacks in spite of using histogram in its watermark insertion method. Also the visual transparency is not achieved in the watermarked image. Then in 2008 [3] proposed a method based on watermark embedding for histogram of HSV planes using visual cryptography watermarking. In the scheme first of all the histogram of all the three components i.e. Hue, Saturation and Value are obtained of the colored image to be watermarked. Then the feature vector 'X' is generated which contains the largest values from the corresponding three histograms respectively, i.e. the values of 'X' are determined by the some threshold value. Only the values greater than threshold values were taken. The size of the watermark chosen is less than or equal to the size of vector 'X'. Then the watermark is inserted by using Hwang's method of cryptography [4]. In the above defined techniques histogram was used to find out the appropriate area for watermark insertion. The area selected was such that it affects the visual perception of the image least or to provide good results against various attacks. The results of technique [1] show that it is robust against various attacks but the major problem prevailing in the technique was its perceptual transparency. The changes in the watermarked image were visible and it is required to perform some image enhancement operation (like histogram equalization) to make the image perceptually same as the original image. The problem of this visual transparency was resolved by technique [3]. Appropriate area for watermark insertion was chosen in reference to some pre defined threshold value from the histogram of Hue, saturation and value component of colored image. The experimental results of the above technique shows that extracted watermark after applying various attacks were not of very good quality (evident from experimental results discussed in the later section).

## II. Proposed Algorithm

**Insertion Mechanism:** The insertion of watermark is performed in the transformed domain. The proposed technique employs the dual domain mechanism making use two transformations i.e. Discreet Cosine Transform (DCT) and Discreet Wavelet Transform (DWT). Inserting watermarks in the LL band increases the robustness of watermark. Hence in the proposed technique we have inserted watermark in the LL – sub band region [5]. Now that we have got the transformed co efficient on which we could insert the watermark but still the question is that how we will change these co efficient to insert the watermark information. We also need to keep in mind that we need to extract the watermark later for the purpose of authentication. Also this decision would decide whether the technique is blind or non-blind. The method employed for inserting watermark is 'Singular Value Decomposition'. Previously many grey level watermarking schemes was proposed inserting the watermark using singular value decomposition. In the classical SVD watermarking approaches the singular values of watermark was inserted into the singular values of the original image. Now at the time extraction only singular values of the watermark




DOI: 01.IJNS.02.03.45

could be extracted. So, the 'U' and 'V' matrixes of the watermark were used as the keys. This procedure is depicted below: The below figure shows the magnified image which is being used as a key. This picture is not as it is used as a key. It is the image formed by multiplication of 'U' and '$V^T$' of watermark image which will be used as keys. But from the above figure it could be clearly make out that the key is very much similar or resemblance to the watermark image. If the watermark image is used as a signature for verification and authentication purposes we could say that only very little information is inserted and the rest of the information is used a key. To overcome the above problem a variation to the above technique is used in our proposed technique [6]. In this variation the singular values of watermark are inserted but the whole watermark is inserted in the singular values. Now we have got the singular values of original watermark on which watermark is being inserted. From this inserted singular values its singular value decomposition is again computed. Now the resultant 'U' and 'V' matrixes are used as keys and new 'S' matrix is used for rebuilding the watermarked image. This procedure is shown in Fig. 2

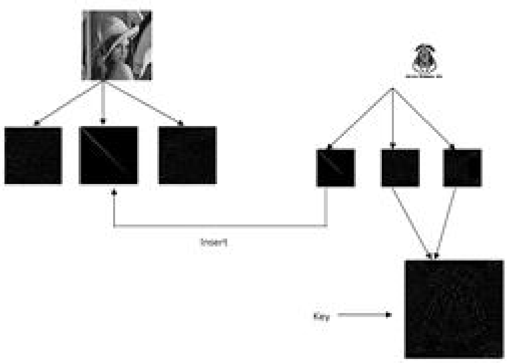



Fig. 1 Classical SVD Technique. Original Image decomposed into U, S and V matrixes and so as watermark image. 'S' of watermark is inserted into 'S' of original image and 'U' and 'V' of watermark is used key for extraction.

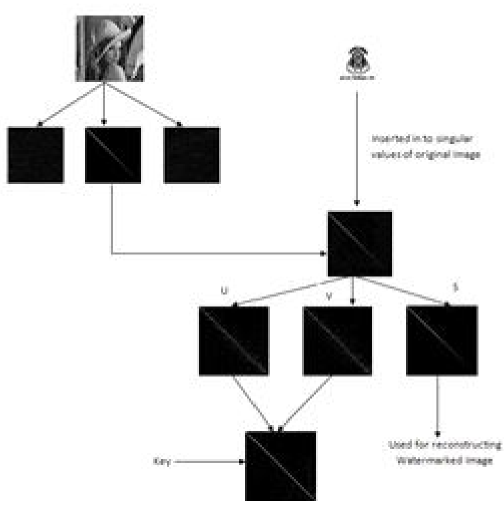



Fig. 2 Variation of classical SVD technique.

From the above two figures we could clearly see the difference between the keys in both the approaches. Clearly, the later one is much secure approach. The key in the later one doesn't convey any information about the shape and geometry of the watermark. This is clearly due to the fact that now much bigger information of watermark is inserted into the original image. And then the decomposition (SVD) is performed to get the singular values and key.

*Algorithm*

The full insertion algorithm is divided into two procedures. First procedure finds out the appropriate area for inserting the watermark. Second is the insertion procedure.

*Procedure 1*

- Convert RGB image of size N × N into HSV color format.
  $Image_{(H, S, V)} = Convert\ (Image_{(R, G, B)})$
- Divide the two – dimensional matrixes Hue and Value into non overlapping blocks of size N/4 × N/4 i.e. 16 blocks each.
- For Hue matrix block compute average hue value for each block as follows:

  $$\frac{1}{a \times b}\sum_{i=0}^{b-1}\sum_{j=0}^{a-1} Hue(i,j)$$

- For each 'Value' matrix block compute the texture value as follows:

  $$\frac{1}{a \times b}\sum_{i=0}^{b-1}\sum_{j=0}^{a-1}(\mathrm{Value}(i,j) - \mu(i,j))^2$$

  $$\text{Where } \mu(i,j) = \frac{1}{a \times b}\sum_{i=0}^{b-1}\sum_{j=0}^{a-1} Value(i,j)$$

- Compute for each Texture value
  1 – Texture
- Compute the mean for each block
  Mean_of_each_block = Mean (Average Hue, Texture)
- Sort the blocks in descending order of their mean value of the 'Value' matrix.
- For first four blocks in sorted list compute DCT (8 × 8 Block wise) of each block.

  $$\sum_{i=1}^{4}(DC)_i = \mathrm{DCT}\ ((\mathrm{Block})_i)$$

- Compute DWT of DCT co efficients of each of the four blocks.

  $$\sum_{i=1}^{4}(LL, HL, LH, HH)_i = \mathrm{DWT}\ ((\mathrm{DC})_i))$$

- Go to Procedure 2.

*Procedure 2*

- Take the watermark image 'W' of size N/4 × N/4.
- Compute DCT (8 × 8 Block wise) of watermark.
  WC=DCT (W).
- Divide the 'WC' into four non - overlapping blocks of size N/8 × N/8.
- Take the LL – band of each of the four block's DWT co efficients compute SVD.

  $$\sum_{i=1}^{4}(U,S,V)_i = \mathrm{SVD}((\mathrm{LL})_i)$$

- Insert each block of 'WC' into each of the four singular values computed above by the SVD method defined in previous section (Variation to classical SVD scheme).




DOI: 01.IJNS.02.03.45

- o Reconstruct the image by following these steps
  - Multiply ‘U’, ‘$S_{Changed}$’ and ‘V’ to get back four LL – bands.

$$\sum_{i=1}^{4}(LL_{changed})_i = \sum_{i=1}^{4} ((U * S_{Changed} * V)_i)$$

  - Get back modified DCT co efficients for each block by taking inverse DWT.
  - Compute the inverse_DCT (8 × 8 Block wise) for each of the four blocks to get modified blocks.
  - Rearrange the blocks to get modified ‘Value’ matrix.
- o Convert the HSV color format watermarked image into RGB color format
  $Watermarked\_Image_{(R,\ G,\ B)}$ = Convert ($Watermarked\_Image_{(H, S, V)}$)

**Watermark Extraction Algorithm:** the following is the algorithm to extract the watermark:

- o Apply the procedure 1 to the image from which watermark to be extracted.
- o Compute the SVD of LL – sub band of each of the four blocks

$$\sum_{i=1}^{4}(U, S, V)_i = SVD((LL)_i)$$

- o From each of singular values compute the compute the inserted blocks with the help of key

$$\sum_{i=1}^{4}((Inserted_{Block})_i) = \sum_{i=1}^{4}(UK * S * VK^T)_i$$

Where ‘UK’ and ‘VK’ are the ‘U’ and ‘V’ components which are used as key to extract watermark.

- o For each of the inserted block compute the blocks of information inserted by following relation

$$\sum_{i=1}^{4}((Extracted\_Information)_{ij} = \sum_{i=1}^{4}(Extract(Inserted_{Block})_i)$$

- o Combine the four blocks of size N/8 × N/8 to form a DCT co efficients image of size N/4 × N/4.
- o Compute the inverse DCT (8 × 8 Block Wise) of resultant image to get the extracted watermark.

## III. Results and Discussion

The performance of the above technique is tested in Mat lab 7.0 software in Microsoft Windows xp with Intel Pentium 4 CPU 3.06 GHz and 512 MB memory. The result evaluation is performed by taking the colored image (24 bits / pixel resolution) of size 512 × 512 and watermark image of size 128 × 128. The watermark image is chosen to be grayscale i.e. of 8 bits / pixel resolution. Following are the inputs and assumptions made during the testing of the technique. The metric used to evaluate the performance of proposed technique is NCC. The NCC values of the extracted watermark are computed with the original watermark image. Below figure shows the images used as original and watermark image.

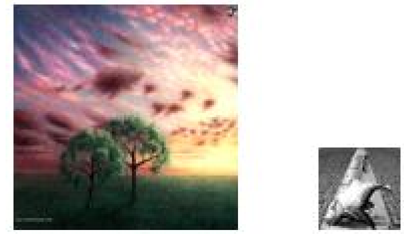


Fig. 3 Original Image and Watermark Image

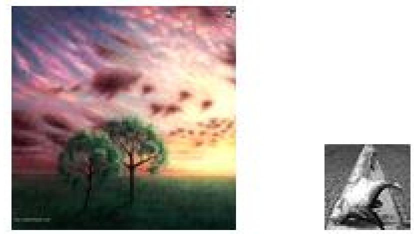


Fig. 4 watermarked Image and extracted watermark from it


Fig. 5 Extracted watermark from Compressed watermarked Image (a )JPEG 60% (b) JPEG 30%





DOI: 01.IJNS.02.03.45

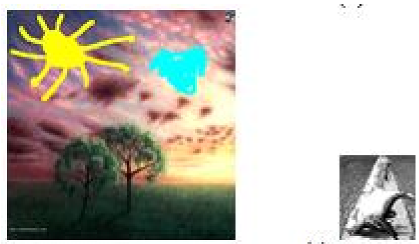



Fig. 6 Attacked watermarked image and extracted watermark from then. (a) White Gaussian noise. (b) Salt & pepper noise (c) Speckle noise. (d) Histogram Equalization. (e) Modification

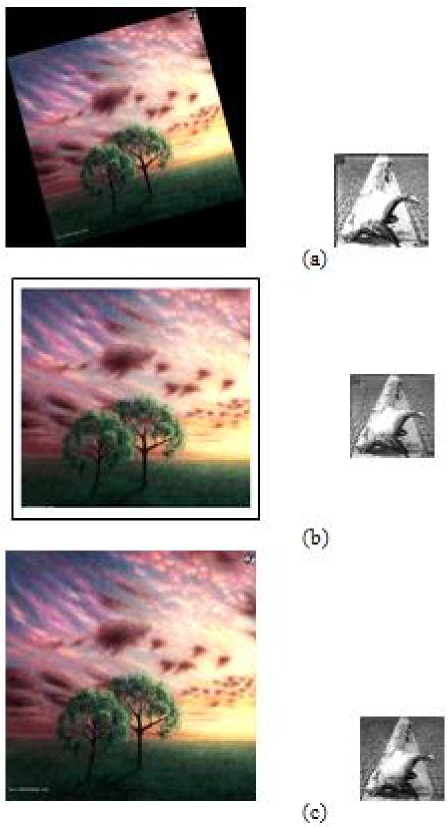


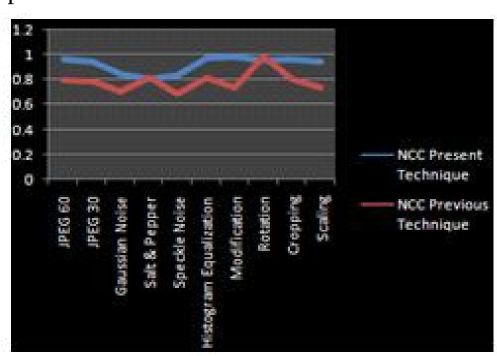

Fig. 7 Geometric Attacked watermarked image and extracted watermark form them. (a)rotation. (b) Cropping. (c) Scaling (2:1)

The results with NCC values for the above defined attacks are given in below Table 1 and also comparison with technique [3] is listed. The reason because the technique provided good results for compression attack is the use of DCT in the insertion mechanism. The DCT is computed ($8 \times 8$ block wise) of both watermark image and blocks of original image. Since due to this the most non lossy or relevant information of both watermark and original information get concentrated on upper left corner and hence most relevant watermark information is inserted into the region which is least vulnerable to JPEG compression. The selection of LL – band of four DWT frequency band has resulted in withstand of image processing attacks by watermark. LL – band represents the lower frequency components of the signal which is most sensible to human visual system but is capable of providing the highest robustness (robustness is inversely proportional to the perceptual transparency). But since already the technique has worked on the HVS to find out the area of image which least sensible to human eyes (in Procedure 1) and also the insertion mechanism employs the use of SVD whose major property is that slight changes in singular values does not affect the perceptual transparency of the image, thus we could chose LL – band to gain high robustness without making compromises with the perceptual transparency. This is the reason why we have preferred the use of HSV color model because HSV color model is the most closely related color model with Human Visual System. In the technique while extracting watermark first step is to find out the area of image where the watermark is inserted based upon the texture and Hue of the image. After applying the geometric attacks when watermarked image will be searched for those areas, then in spite of applying the geometric attacks algorithm will find those area only in which the watermark information exist. In geometric attacks the dimension of area in which watermark is inserted night got changed but the texture and hue of the area will not be changed.

TABLE I

| Attacks | NCC Present Technique | NCC Previous Technique |
|---|---|---|
| JPEG 60 | 0.9693 | 0.7930 |
| JPEG 30 | 0.9426 | 0.7882 |
| Gaussian Noise | 0.8445 | 0.7045 |
| Salt & Pepper | 0.8033 | 0.8171 |
| Speckle Noise | 0.8392 | 0.6869 |
| Histogram Equalization | 0.9783 | 0.8185 |
| Modification | 0.9880 | *0.7400* |
| Rotation | 0.9580 | 0.9844 |
| Cropping | 0.9682 | 0.8086 |
| Scaling | 0.9502 | 0.7348 |

But considering the overall results our technique proves to be more robust than the previous one. Considering the other attacks it could be observed that there is a huge difference between their NCC values. To show the differences in results of both techniques the below two graphs are being plotted i.e. Graph 1.




GRAPH 1

## CONCLUSION

The proposed technique emphasizes on finding the perceptually most significant area of the image to which Human Visual System is least sensitive. In addition to




DOI: 01.IJNS.02.03.45

perceptual transparency high robustness is achieved by inserting the watermark in dual transformed domain i.e. by using DCT and DWT. Further both robustness and perceptual transparency is increased by making use of 'Singular Value Decomposition'. The only disadvantage of the proposed technique is the diagonal line which is being visible in the many extracted watermarks from attacked watermarked image. The loss of information in diagonal could be explained as. The watermark is inserted into the singular values, this means that the diagonal information of watermark get inserted into singular values. When watermarked image is reconstructed from that than watermark's diagonal information get spreaded throughout the image. Due to this, diagonal information is lost when attacks applied to the image which affects the whole image.

## REFERENCE

[1] Color Image Watermarking in HIS Space by Dinu Coltuc and Philippe Bolon (0-7803-6297-7/00 2000 IEEE).

[2] D. Coltuc, Ph. Bolon, "Regional Watermarking in Spatial domain", European Conference on Signal Processing EUSIPCO '2000, Tampere, Finland, 2000.

[3] "HSV Image Watermarking Scheme Based upon Visual Cryptography" by Rawan I. Zaghloul, Enas F. Al-Rawashdeh, PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY VOLUME 34 OCTOBER 2008 ISSN 2070-3740.

[4] R. Hwang, A digital Image Copyright Protection Scheme Based on Visual Cryptography, Tambang Journal of science and Engineering, vol.3, No.2, pp. 97-106 (2000).

[5] "Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks" by, Saraju P. Mohanty and Bharat K. Bhargava, proceedings of ACM Journal Name, Vol. V, No. N, February 2008, Pages 1–24 (ACM 0000-0000/2008/0000-0001).

[6] Liu, R. and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. on Multimedia*, Vol. 4, No. 1 March 2002.




DOI: 01.IJNS.02.03.45